

NEWARK AND SHERWOOD DISTRICT COUNCIL

DATA PROTECTION POLICY

1. Introduction.

Newark and Sherwood District Council ('the Council') aims to ensure that personal information is treated lawfully and correctly. The lawful and correct treatment of personal information is extremely important in maintaining the confidence of those with whom the Council deals and in achieving its objectives.

The Council fully endorse and adhere to the Data Protection principles set out below:-

THE EIGHT DATA PROTECTION PRINCIPLES

Personal Information:

- shall be processed fairly and lawfully and shall not be processed unless specific conditions are met;
- shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose of those purposes;
- shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed;
- shall be accurate and where necessary kept up to date;
- shall not be kept for longer than is necessary for that purpose or those purposes;
- shall be processed in accordance with the rights of data subjects under the Act;
- appropriate technical and organisational measures will be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data;
- shall not transfer personal data to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

2. Policy Aim

To ensure the Council complies with all relevant legislation and good practice to protect all of the personal information that it holds.

3. Policy Objectives

To achieve the overall aim the Council will:

- 3.1 Provide adequate resources to support an effective corporate approach to Data Protection.
- 3.2 Respect the confidentiality of all personal information irrespective of source.
- 3.3 Publicise the Council's commitment to Data Protection.
- 3.4 Compile and maintain appropriate procedures and codes of practice.
- 3.5 Promote general awareness and provide specific training, advice and guidance to its staff at all levels and to its Members to ensure standards are met.
- 3.6 Monitor and review compliance with legislation and introduce changes to policies and procedures where necessary.

4. Processing of Information:

The Council, through appropriate management controls will, when processing personal information about any individual:

- 4.1 Observe fully the conditions regarding the collection and use of information and meet the Council's legal obligations under the Data Protection Act 1998 ('the Act').
- 4.2 Collect and process appropriate information only to the extent that it is needed to fulfil operational needs or to comply with any legal requirement.
- 4.3 ensure that the individual about whom information is held can exercise their rights under the Act, including:-
 - 4.3.1 the right to be informed that processing is being undertaken
 - 4.3.2 the right to prevent processing in certain circumstances
 - 4.3.3 the right to correct, rectify, block or erase information, which is regarded as incorrect information.
 - 4.3.4 the right of access to personal information

5. Fair Obtaining/Processing

Individuals whose information is collected by the Council must be made aware at the time of collection of all the processes that data may be subject to. No manual or automatic processing of an individual's personal information should take place unless reasonable steps have been taken to make that individual aware of that processing. Individuals must also be informed of likely recipients of their information, both internal and external, and also be given details of who to contact in order to query the use or content of their information.

6. Data Uses and Purposes

- 6.1 All processing of personal data must be for a purpose that is necessary to enable the Council to perform its duties and services, and which has been notified by the Council to the Information Commissioner. Personal information should only be processed in line with those notified purposes.
- 6.2 No new processing should take place UNTIL the Information Commissioner has been notified of the relevant purpose AND the data subjects have been informed and, in the case of sensitive data, their consent obtained. All new occurrences of, or future developments for, processing of personal data must therefore be reported to the Policy Officer (Access to Information), who is responsible for maintaining Council's Data Protection notifications.
- 6.3 All personal data should be regarded as confidential and its security protected accordingly. This also applies when Council information is being processed at employees' homes. Employees should only remove personal information from a Council office with the authority of their line manager, head of service or the Chief Executive. Any misuse, loss or unauthorised disclosures while the information is in their control may result in disciplinary proceedings. Information held by the Council must not be used for unauthorised non-Council purposes.
- 6.4 Personal Information should only be disclosed to persons (internal and external) who are listed for the purpose concerned in the Council's current notification OR where their authority to receive it has been explicitly established, e.g. where the information is required by the police for the prevention and detection of crime.

7. What counts as Personal Information?

This is any information held by the Council about a living individual, from which that individual can be identified. For example, this will include :

- A name and address,
- information attached to a reference number that could be used to identify someone
- a company e-mail address if it includes a person's name.

8. Data Quality

Information processed should not be excessive or irrelevant to the notified purposes. Information must be held only for so long as is necessary for the notified purposes, after which it should be deleted or destroyed in accordance with the councils Retention and Disposal schedule. Whenever information is processed, reasonable steps should be taken to ensure that it is up to date and accurate.

9. Organisational Responsibilities and Security

The Council is obliged under the Act to ensure that all appropriate technical and organisational measures are taken to safeguard against unauthorised or unlawful processing of personal information and against the accidental loss, damage or destruction of personal information.

- 9.1 All personal information must be kept secure, in a manner appropriate to its sensitivity and the likely harm or distress that would be caused if it was disclosed unlawfully. To ensure that an appropriate level of security is afforded to all information the Council's Information Security policy will be adhered to at all times.
- 9.2 Everyone managing and handling personal information will be appropriately trained to do so.
- 9.3 All members of staff have a duty to follow this Policy and procedures and to co-operate with the Council to ensure that the aim of this Policy is achieved.
- 9.4 Disciplinary action may be taken against any member of staff who fails to comply with or commits a breach of this Policy.
- 9.5 It is the duty of individual members of staff to ensure that personal information held by them is dealt with in accordance with the Act.
- 9.6 Suitable measures should be taken to ensure that any processing of personal data carried out by a third party on behalf of the Council complies with the Principles of the Act and this Policy. Similarly, when the Council is processing personal information on behalf of a third party it will need to demonstrate that the information is subject to the same standard of care.

Author:	Steve Bramall
Document Status	Approved
Approval	
Approved By:	K White
Position:	HLDS&HR
Approval Date:	27.11.08
Version:	1.0